DEY 3/29/07

Please replace the paragraph on page ~~24~~ 23, line ~~21~~ 11 through ~~page 25~~, line ~~8~~ 21 with the following amended paragraph:

Other approaches for key exchange that are suitable for use in embodiments of the present invention are disclosed in co-pending application Ser. No. ~~NUMBER1~~ 09/393,410, filed on ~~the same date as this application~~ September 10, 1999, and naming as inventor Sunil K. Srivastava, and entitled "OPERATIONAL OPTIMIZATION OF A SHARED SECRET DIFFIE-HELLMAN KEY EXCHANGE AMONG BROADCAST OR MULTICAST GROUPS," the entire disclosure of which is hereby incorporated by reference as if fully set forth herein, and in co-pending application Ser. No. ~~NUMBER2~~ 09/408,420, filed on ~~the same date as this application~~ September 10, 1999, and naming as inventor Sunil K. Srivastava, and entitled "PROCESSING METHOD FOR KEY EXCHANGE AMONG BROADCAST OR MULTICAST GROUPS THAT PROVIDES A MORE EFFICIENT SUBSTITUTE FOR DIFFIE-HELLMAN KEY EXCHANGE," the entire disclosure of which is hereby incorporated by reference as if fully set forth herein.

SPECIFICATION AMENDMENTS

DEB 3/29/07

Please replace the paragraph on page 5, line ~~21~~ 17 through ~~page 6,~~ line ~~1~~ 21 with the following amended paragraph:

Alternatively, Diffie-Hellman is used to do a point to point communication with the CA or KDC, and the CA or KDC can give out a group session key without using the binary tree approach. All nodes get the same session key using N-1 point to ~~pint~~ point messages. These two approaches are orthogonal and can be combined for optimization.

DEB 3/29/07

Please replace the paragraph on page 6, line ~~16~~ 12 through page 7, line ~~6~~ 1 with the following amended paragraph:

A binary tree approach is disclosed in co-pending application Ser. No. ~~NUMBER3~~ 09/407,785, entitled "METHOD AND APPARATUS FOR CREATING A SECURE COMMUNICATION CHANNEL AMONG MULTIPLE ~~PROXY MULTICAST~~ EVENT SERVICE NODES," filed concurrently herewith, and naming as inventors Sunil K. Srivastava, Jonathan Trostle, Raymond Bell, and Ramprasad Golla, the entire disclosure of which is hereby incorporated by reference as if fully set forth herein. The binary tree approach described therein makes it possible to scale a secure communication system to large multicast groups, with less overhead involved in transmission of new group session keys when members join in a multicast group. Advantageously, each affected member does only $\log_2 N$ decryption operations; further, when a member joins or leaves, the central group controller, which acts as a group membership coordinator, sends only a subset of keys to existing group members on an affected tree branch. All keys that are affected can be sent, ideally, in one multicast or broadcast message, and only keys that correspond to a particular node will be decrypted by that node.